

DECLARATION IN SUPPORT OF CIVIL COMPLAINT FOR FORFEITURE

I, Martez Simpson, a Special Agent with the United States Secret Service (“USSS”), being first duly sworn, hereby state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I have been employed as a Special Agent with the USSS since March 2022 and am currently assigned to the Jackson Resident Office in Jackson, Mississippi. As part of my law enforcement duties, I am statutorily charged with investigating wire fraud, bank fraud, false statements regarding bank fraud, fraud in connection with major disaster or emergency benefits, fraud, and related activity in connection with electronic mail, major fraud against the United States, money laundering, and cybercrimes, as well as other criminal cases. Prior to my tenure as a Special Agent, I worked in law enforcement with the state of Mississippi for six years. I have a bachelor’s degree in criminal justice from Old Dominion University.

2. The information contained in this Declaration is based upon my personal knowledge and on information I obtained from other law enforcement officials. Since this Declaration is being submitted for the limited purpose of establishing the basis for this civil forfeiture action, as set forth herein, I have not included each and every fact known to me concerning this investigation, but only facts that I believe are necessary to establish—more likely than not—that the Binance.com wallet 16LFVNKLReJ3qXAN1J9q9sYortqx6vTWqt (the “Binance wallet”) was used to receive the proceeds of and/or facilitate violations of 18 U.S.C. §§ 1343 (Wire Fraud) and/or 1956(a)(2) (International Money Laundering), and that the funds in the wallet are therefore subject to civil and criminal forfeiture to the United States.

3. I have been personally involved in the investigation of this matter. This Declaration is based in part upon my conversation with victims and sources and upon my examination of various transcripts, reports, and other records. When the contents of documents

and statements of others are reported herein, they are reported in substance and part unless otherwise indicated.

4. There is probable cause to believe the funds in the Binance wallet were derived from proceeds traceable to violations of specified unlawful activities, specifically, proceeds traceable to violations of 18 U.S.C. §§ 1343 and/or 1956(a)(2). Furthermore, the Binance wallet was involved in and used to facilitate violations of 18 U.S.C. § 1956(a)(2). As such, the funds contained in the Binance wallet are subject to forfeiture pursuant to 18 U.S.C. §§ 981(a)(1)(A), (C), and (D).

PROPERTY TO BE SEIZED

5. The Defendant Property (hereafter “the Binance wallet”) sought for forfeiture includes the following asset:

Asset ID	Asset Description
24-USS-000174	All funds located in Binance.com wallet 16LFVNKLReJ3qXAN1J9q9sYortqx6vTWqt ¹ , created on January 30, 2022, by an Indian national named Sikandar Azmi, approximately 0.447893442024797 cryptocurrency worth approximately \$29,788.29 ²

which was seized on June 5 and 18, 2024, pursuant to a federal seizure warrant, from Nest Services Limited (trading as Binance) in Mahe, Seychelles.

¹ This Binance wallet “address” is a unique identifier used to send and receive cryptocurrencies on the Binance exchange. Binance.com, which is not available in the United States, offers more features, a wider breadth of cryptocurrencies, and lower fees than Binance.US, and is used for account holders with an IP address in the United States.

² As of June 20, 2024, the Binance wallet contained 50.68862 OMNI coins valued at \$1,008.42, 66,588.950 AMP coins valued at \$454.13, and 27,953.339883 USDT coins valued at \$27,943.41.

FACTS AND CIRCUMSTANCES

6. On or about April 18, 2024, Victim #1 (“V1”) received an email in her personal email account, purportedly from McAfee, Inc., indicating that \$723.64 was being taken from her bank account. This email was part of a phishing scam, a type of online scam that targets consumers by sending them an e-mail that appears to be from a well-known source, such as an internet service provider or a bank. V1 contacted the phone number listed in the email, (828) 357-4196.

7. After calling the phone number, V1 spoke with an unknown individual (“UI”)³, who she believed to be a McAfee employee. The UI directed her to fill out certain forms on her computer. As she did so, the UI gained remote access into V1’s computer. Using command prompt entries, the UI convinced V1 that, rather than the \$723.64 that the email had indicated was improperly taken out of her bank account, her banking data indicated a \$77,723.64 amount was refunded. The UI informed V1 that because the wrong amount was refunded to the account, V1 needed to physically withdraw money from the bank and deposit the money into a Bitcoin ATM.

8. Based on my training and experience, I know this is tactic fraudsters use to get victims to access their bank accounts and deposit money into Bitcoin ATMs. The UI demanded that V1 follow his instructions, or she would not get her money or control of her electronics back. V1 was instructed to stay on the phone and travel to her bank to withdraw \$15,000.00 in cash. V1, who was convinced the UI had access to her mobile phone and email account, believed she would regain access of her electronics if she followed the UI’s instructions.

³ It is not clear whether all the acts committed by a UI were committed by the same individual.

9. V1 withdrew \$15,000.00 in cash from the Trustmark National Bank – Castlewoods, located at 5627 U.S. Highway 25, Flowood, Mississippi. V1 was instructed to go to two separate Bitcoin ATM locations. The first ATM transaction occurred at 5315 I-55 N, Jackson, Mississippi; the second at 3006 Greenfield Road, Pearl, Mississippi. V1 was instructed to email the Bitcoin tracking codes to tdbearry24@gmail.com. When she did so, someone replied with a quick-response (“QR”) code for the Bitcoin transactions. Using the QR code, V1 initiated the two following transactions at the two above-referenced Bitcoin ATMs:

Transaction #1: V1 converted \$6,032.05 of her money into Bitcoin, which was sent to the receiving address: 34b3mxp8bs6dtotfAozcRcWFjLrGmXZuET. Thereafter, the UI forwarded the Bitcoin to the Binance wallet.

Transaction #2: V1 converted \$4,939.81 of her money into Bitcoin, which was sent to the same receiving address. Thereafter, the UI forwarded the Bitcoin to the Binance wallet.

10. V1’s bank advised her that she may have been the victim of fraud, and V1 contacted the Mississippi Attorney General’s Office, who handed her complaint to one of its investigators—USSS Task Force Officer (“TFO”) Nick Sprowles. TFO Sprowles spoke with V1 and conducted chain analysis on the above-mentioned transactions. Chain analysis involves examining blockchain data such as transactions, trades, and wallet address holdings to understand the actions of market participants on respective blockchains in real time. During the chain analysis, the above-mentioned transactions were traced to the suspect’s Bitcoin address: 16LFVNKLReJ3qXAN1J9q9sYortqx6vTWqt.

11. TFO Nick Sprowles issued a request to Binance.com for account information and ownership verification of the Binance wallet and to freeze movement of funds contained in the wallet. Binance.com acknowledged the request and froze the funds for a seven-day period. A

representative from Binance advised that the frozen account/wallet contained just less than \$30,000.00. TFO Sprowles also contacted me to take charge of the investigation.

12. On April 22, 2024, V1 gave TFO Sprowles and me access to her email account, but we were not able to locate the phishing email that had been sent to V1. Fraudsters often remotely access the computers of their victims and delete the email completely from the victim's system, to destroy evidence of their crime.

13. On April 23, 2024, Binance provided Know Your Customer ("KYC") information for the Binance wallet, which revealed that the account was created on January 30, 2022, by an Indian national using the name Sikandar Azmi ("Azmi"). The KYC information also revealed Azmi's date of birth, phone number, and email address. Binance informed me that the wallet held approximately \$29,788.29 worth of cryptocurrency.

14. On April 29, 2024, an unknown male, who I believed to be Azmi⁴, contacted me by phone, using the phone number: (928) 208-4489, which was registered to Sidartha Christenson, who is deceased. Azmi asked why his Binance account has been frozen. I identified myself as a Special Agent with the United States Secret Service and asked Azmi if he knew why his account has been frozen. Azmi responded that it had been frozen for fraudulent activity and told me that he purchased Bitcoin from an unknown person through Binance, but that once he received the Bitcoin, he was unable to convert it into "USD,"⁵ which led Azmi to realizing that his account had been frozen. I asked Azmi about the unknown person from whom he had purchased the Bitcoin, and Azmi said a lot of unknown people contacted him to trade

⁴ For clarification purposes, I am referring to this unknown person as Azmi herein.

⁵ It was unclear whether Azmi meant U.S. Currency, USDC cryptocurrency (preferred for those who value transparency and a cryptocurrency with a stable value), or USDT cryptocurrency (also having a stable value, preferred for liquidity and investing in a higher volume of cryptocurrency).

Bitcoin. Azmi was adamant that he doesn't know these people, insisting that he was just a trader. I believe Azmi was using the conversation to "fish" for information regarding the frozen account and become better at this type of cryptocurrency scheme.

15. On April 24, 2024, a magistrate judge granted a federal seizure warrant for the Binance wallet pursuant to 18 U.S.C. § 981(b) and 21 U.S.C. § 853(e) and (f) by 18 U.S.C. § 982(b)(1) and by 28 U.S.C. § 2461(c). Although the warrant was served on Binance that same day, a backlog in Binance's legal department led to the wallet contents not being received by the government until June 5, 2024, and June 18, 2024.

16. The investigation into the source of the remaining money deposited into this Binance wallet is ongoing. Preliminary information indicates that all of the funds are the result of similar fraud schemes, but the United States is waiting for companies to respond to several subpoenas for records pertinent to this case.

CONCLUSION

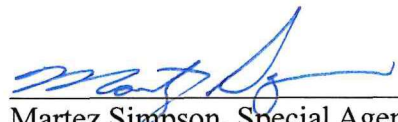
17. Based upon my training and experience, and the facts and circumstances outlined in this Declaration, I reasonably believe that the Binance wallet is subject to civil forfeiture pursuant to 18 U.S.C. §§ 981(a)(1)(A), (C), and (D), on the grounds that it represents property which constitutes or is derived, directly or indirectly, from proceeds traceable to 18 U.S.C. § 1343 (Wire Fraud) and/or was involved or used, or intended to be used, in any manner or part, to commit, or facilitate the commission of violations of 18 U.S.C. § 1956(a)(2) (International Money Laundering).

18. The results of this investigation support my reasonable belief that the government can meet its burden of proof that the Defendant Property is directly related to and/or derived

from the wire fraud and/or international money laundering described herein. This determination was made on the facts and circumstances presented above.

19. I declare, pursuant to 28 U.S.C. § 1746, that the foregoing is true and accurate to the best of my knowledge and belief.

Executed this 5 th day of July 2024,



Martez Simpson, Special Agent
United States Secret Service